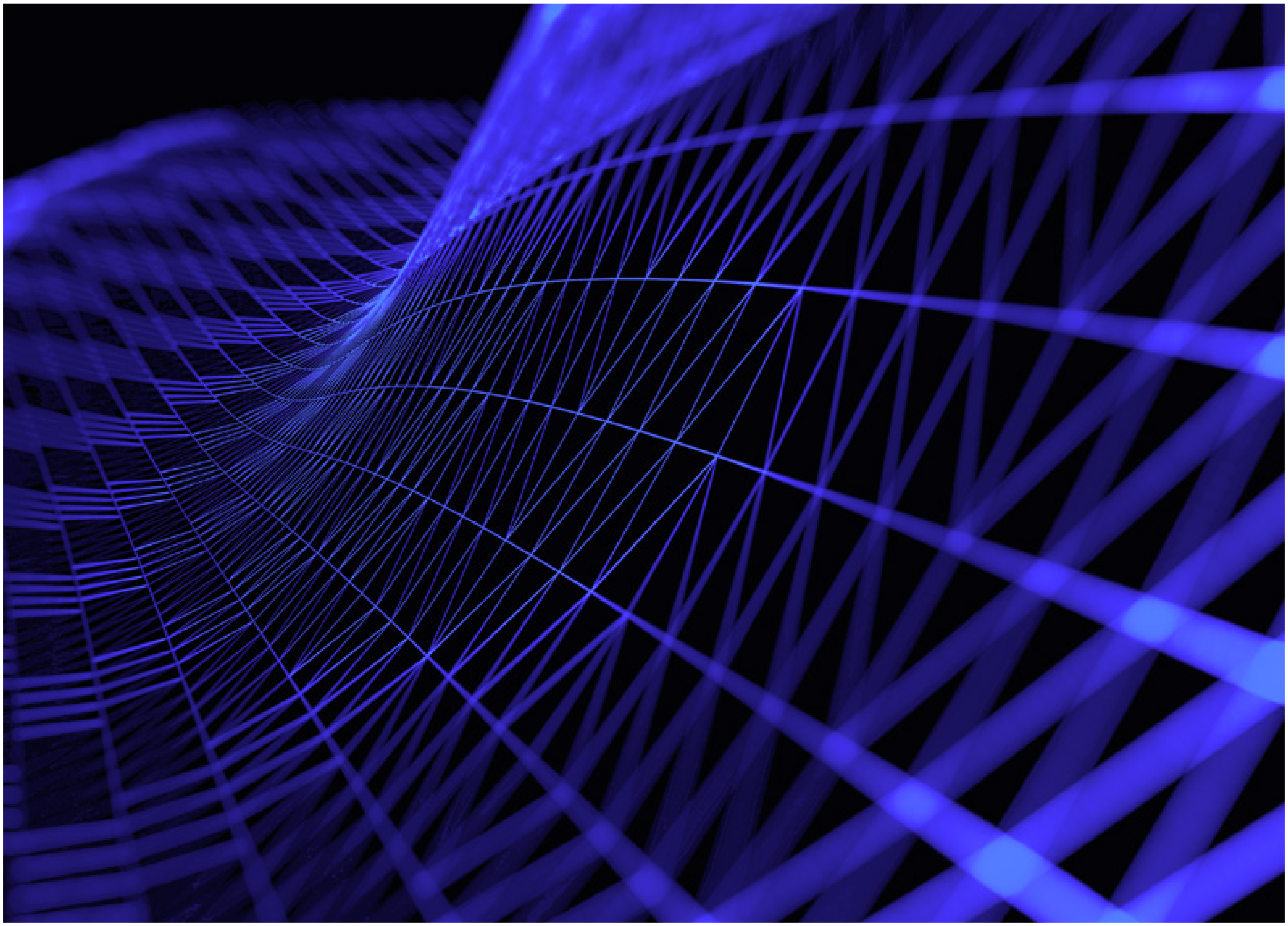
Secureworks®

WHITE PAPER

Outmaneuvering Advanced and Evasive Malware Threats



The tactics of threat actors are evolving. Today, businesses of all sizes are subject to highly targeted attacks that rely on specially modified malware. Wielded by threat actor's intent on stealing trade secrets, intellectual property and other high-value data, these attacks evade detection by traditional security controls and even some sandboxing technologies built to dynamically analyze malware.

Combatting these advanced and evasive malware threats and resolving breaches consume significant amounts of remediation time and security budgets. Security teams need to rethink their people-process-technology mixes and strengthen them to defeat emerging threats, which are on the upswing.

According to Ponemon Institute's "2018 State of Endpoint Risk" report[1]:

- Sixty-three percent of respondents reported a significant increase in the number of malware incidents targeting their endpoints – up from fifty-eight percent in the year prior.
- Thirty-five percent of endpoint attacks in 2018 were fileless, using techniques like macros, scripting engines, in-memory execution etc. This marks a significant increase from 2017.
- The cost of successful attacks has increased from an average of $5 million to $7.1 million. Costs due to the loss of IT and end-user productivity and theft of information assets have increased.

The inability to identify and resolve these threats rapidly can result in publicity-generating breaches, business downtime, financial losses, and loss of competitive advantage. But a new approach — an innovative combination of threat intelligence and next-generation sandboxing — can help businesses enhance their security postures to outsmart and outmaneuver attackers and to resolve breaches in less time.

A Business Problem, Not a Malware Problem

VirusTotal, the popular online virus-, malware- and URL-checker, averages 1.2 million file submissions per day– 900,000 of them distinct and new to VirusTotal.

The threat actors behind malware may target a specific business and set of data, and they do their research. They identify the weakest spots in an organization's security posture and may use publicly available data to identify potential targets for spear-phishing campaigns. The threat actors also implement techniques and technologies to override security protections such as antivirus (AV) software, intrusion detection systems

(IDS), intrusion prevention systems (IPS) and even some advanced threat protection systems built to dynamically isolate and defuse malware.

With so-called "evasive" threats, the threat actors customize the malware to the target organization and then couple it with technologies to evade detection while the malware compromises the systems. For example:

- Some malware detects that it has been redirected to a sandboxed or virtualized environment, enabling attackers to quickly modify their approaches.
- Malware may introduce timing delays to "sleep" for a defined period while a sandbox is likely monitoring, to trick the system into interpreting the malware as benign code.
- Malware may efficiently target only key systems to avoid being flagged by the general security community. For example, malware targeted at point-of-sale systems is smart enough to move on if it encounters a non-POS system.
- Malware has targeted IoT technology as well, with documented cases of specific unpatched routers being compromised and their CPUs harnessed to mine cryptocurrency (Crypto mining malware grew 4,000% in 2018.)

For businesses, the right mix of people, processes and technology has always been important in effective information security. Today, it's imperative that all businesses adjust this mix to deal with more complex threats.

Signature-based detection and resolution technologies alone are not sufficient against most evasive attacks. Security teams need the skills and processes to develop context on unknown threats to understand what the threat really means: technology itself won't tell them. Teams need to able to detect, analyze, develop and add context and resolve evasive threats and breaches — fast.

In short, businesses need a different approach that lets them outmaneuver sophisticated threat actors.

Technology to Combat Malware

Sandboxing and next-gen sandboxing solutions provide an advantage over traditional approaches to combatting malware by dynamically detecting and analyzing malware behavior. By doing so, they've become as ubiquitous as a screwdriver in the toolbox of many security organizations.

Sandboxing solutions typically offload and detonate the malware away from the main environment. Unlike traditional IPS solutions, sandboxing solutions can analyze the actual executable content from the Internet. For example, they can flag web scripts that are part of exploit kits or that open potentially malicious email attachments and run potentially malicious executables in a sandbox. Detonating these potential threats captures the malware behaviors; experienced malware analysts can then examine the threat and develop filters and protections based on the behaviors.

There are three technical approaches to sandboxing, offering varying levels of effectiveness.

1. **Virtual-machine (VM) sandboxing** offloads malware to virtual machines that replicate the targeted environment. It provides a lower level of malware- behavior visibility than other solutions. As a result, it traditionally has offered higher resistance to subversion by malware. However, malware creators have now designed payloads to trick some VM sandboxing environments.
2. **OS emulation** emulates the target environment at the operating system level. It provides a higher level of malware-behavior visibility but has low resistance to subversion by malware.
3. **Full-system emulation sandboxing** simulates the target environment at the physical hardware level (CPU and memory) to convince the malware that it is running on the target system's hardware. If offers both a high level of malware-behavior visibility and a high level of resistance to subversion by malware.

People and Processes to Combat Malware

Businesses also need to update their skills and processes to deal with malware. Required skills include:

- Malware analysis and reverse engineering for sorting through the voluminous data on host-based changes generated by sandboxing systems to deduce malware behavior and profile threat actors.
- Low-level knowledge of endpoint platforms (Windows, Android, Linux) for spotting anomalies potentially caused by malware. (Evasive malware can often do significant damage by infiltrating select endpoint systems; as long as the malware doesn't cross any network boundaries, it stays under the radar of host-based detection systems.
- Experience in host-based forensics and related investigative skills to understand the TTPs (tactics, techniques and procedures) of the threat actors.
- Skills for collecting, categorizing and acting on intelligence generated by malware reverse- engineering.

People with these skills have typically spent years honing their skills into tradecraft, making them very much in demand, pricey and difficult to find and retain. They are usually found in the military, government, leading security product vendors and service providers or large commercial companies with advanced security intelligence operations.

While sandboxing solutions have come a long way in automating how security teams respond to malware, the solutions are optimized for detection not resolution. They lack integrated capabilities for analyzing the behavior of malware and of threat actors (via malware analysis and reverse engineering). This gap can delay effective response to a breach, while costs, data losses and negative publicity mount. These solutions need to get smarter at staying ahead of malware.

Unfortunately, it's usually not possible to redeploy current security operations staff. Malware analysis and reverse engineering involves analyzing suspicious objects, binaries and URLs in a very different way from the way one would analyze an alert from a network IDS. Effective malware analysis requires both experience and intuition.

On the process side, businesses need a workflow for malware analysis and intelligence that:

- Triages and analyzes feedback from next-generation sandboxing systems
- Gleans intelligence from the feedback through analysis and reverse engineering
- Creates actionable intelligence for security operations staff
- Captures effective responses, signatures and countermeasures for re-use/refinement

The ultimate goal is to slow down or repel threat actors by forcing them to change their approaches dramatically — not simply change their IP addresses or obtain new domain names.

Threat Intelligence

To combat advanced and evasive threats, businesses need a defense-in-concert strategy informed by threat intelligence.

According to the Commission on Organization of the Executive Branch of the Government (the Hoover Commission): "Intelligence deals with all the things which should be known in advance of initiating a course of action."

Establishing an effective defense-in-concert strategy for advanced and evasive threats involves overcoming two popular misconceptions:

Misconception #1: A single type of threat intelligence is enough.

Reality: A single type – for example, a historical threat database or a community antivirus checker — doesn't provide an adequate vantage point from which to deduce the specific threat landscape facing your organization today and in the future.

The Process: Trained professionals watching the alerts as they come in 24x7, correlating the alerts with what is already known about your environment, including all available threat intelligence, and providing actionable information as soon as possible after a threat is discovered.

Misconception #2: Indicators (domain names, IP addresses, hashes) constitute "intelligence."

Reality: Indicators are good data points but do not provide adequate context for quick and effective threat detection or prevention. Security operations staffs need the ability to use ongoing streams of threat intelligence, as well as the ability to generate and use new intelligence just in time to enrich the context for making critical decisions.

Threat intelligence can strengthen advanced and evasive threat protection at every level of operation:

- Detection: Access to information beyond traditional AV, IDS/IPS and sandboxing system alerts can help speed detection by providing additional vantage points on a threat.
- Context and Diagnosis: A threat intelligence provider that studies adversaries' behavior across thousands of client installations may have insights or countermeasures that are not available from an individual sandboxing system or addressed by AV signatures.
- Resolution: Combatting attacks and resolving breaches faster requires solid malware analysis and reverse engineering skills, and threat intelligence is critical to these efforts.

Network and Endpoint Visibility Required

An effective approach to advanced and evasive malware must also provide more complete threat detection by integrating with security controls at both the network and endpoint levels.

Network-level systems enable businesses to easily and quickly protect a large number of clients without worrying about endpoint performance impact, system administration overhead or malware tampering with the endpoint client. Endpoint-level systems provide vital additional visibility regardless of how a malware program gets to the endpoint; for example, malware downloaded through HTTPS, files loaded through USB sticks, or data exposed on laptops taken outside the protected perimeter.

In both kinds of systems, the key challenge is accurate malware analysis: proper classification of an unknown binary as malware or a benign file. The optimal strategy is to integrate network monitoring with existing endpoint technology to achieve visibility of the entire environment — and insight into malware execution stack.

Threat intelligence can speed resolution of breaches by helping pinpoint the affected systems, wherever they are. Responding to 12, 13 or 20 affected endpoints instead of all 20,000 can dramatically reduce the cost, time and manpower of responding to a breach — even putting it within the realm of normal IT resources.

A New Approach

Combining threat intelligence with sandboxing technologies can improve the security posture of organizations regardless of their maturity level.

But how to achieve this, given static or declining security budgets and senior management's lack of understanding of the value of advanced and evasive threat protection?

Fortunately, malware-fighting technology continues to evolve. Next-generation systems combine the leading malware-detection and -detonation technology (e.g., full-system-emulation sandboxing technologies that cover CPU to memory) with advanced threat intelligence based on behavioral analysis of threat actors from multiple vantage points across thousands of organizations.

Such capabilities are now offered as hosted services, making them an operational expense (OPEX) versus a capital expense (CAPEX). This makes them affordable for large organizations in key vertical industries targeted by attackers, as well as small to medium-sized businesses with enterprise-class security needs.

All kinds of businesses can benefit:

- Instant expertise: Medium-sized organizations lacking internal malware-fighting skills, processes and personnel can acquire capabilities quickly, fast-tracking their maturity levels.
- Enhanced Security: Organizations unsure of the effectiveness of their current sandboxing systems can complement them with a next-generation solution, without disruptive rip-and-replace.
- Trust & verify: Large organizations that want to bulletproof their advanced and evasive threat protection strategies can quickly deploy next-generation expertise to complement their current systems. They can affordably run two systems side-by-side for performance comparison or validation.

Pulling it Together: A Strategy

It may be impossible to prevent all malware attacks. However, a defense-in-concert strategy that includes the following protections is the best way to combat advanced and evasive threats and recover from breaches faster:

- Advanced threat detection at the network level that is tied to an existing IPS/IDS and firewall.
- Advanced threat detection at the endpoint.
- A forensics readiness program that includes an easily accessible incident response capability. Periodically execute incident response preparation or readiness exercises, establish procedures for accessing critical state information such as system images and store critical log data so that it is available and trustworthy.
- An ongoing employee security awareness program to train and remind employees how to recognize potential threats, including spear-phishing.

Recommendation

Businesses need a well-thought-out security defense layer with the right instrumentation, the right threat intelligence and the right security expertise on staff to minimize the effect of today's advanced and evasive threats. Understanding the behavior of adversarial threat actors is critical to anticipating and responding to attacks and to resolving breaches faster. Telemetry and technology alone can't provide the depth of understanding needed, nor can they produce effective countermeasures. By combining advanced threat intelligence from specialists who study adversarial behavior with the most current detection technology (next-generation sandboxing), organizations will have the best chance at outmaneuvering advanced and evasive threats.

Sources:

[1] Ponemon Institute, "2018 State of Endpoint Risk," October 2018, survey of 660 IT and IT security professionals with involvement in endpoint security.

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States

1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan

Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp